WHAT IS CLAIMED IS:

1. An access control system for use in a data transfer system which transfers data by means of public-key cryptosystem based on a public key certificate issued to an authentication object by a public key issuer authority, the access control system comprising:

a service provider which is an authentication object and which provides services;

a service receiving device which also is an authentication object and which receives services provided by the service provider; and

an access control server which issues to the service receiving device an access permission which identifies a service provider an access to which by the service receiving device is permitted;

wherein the service provider performs, based on the access permission, a decision as to whether an access request by the service receiving device is to be permitted.

2. An access control system according to Claim 1, further comprising:

an access-control-server registration server,

wherein the access-control-server registration server is configured to execute a processing for requesting the

access control server to execute issuance of the access permission, upon receipt of an access permission issuance request from the service receiving device.

3. An access control system according to Claim 1, further comprising:

at least one system holder which is an organization that provides or controls contents usable by a user terminal, contents which enables provision of services, or a service distribution infrastructure;

wherein the system holder is configured to administrate the service provider and the service receiving device and to treat the service provider and the service receiving device as authentication objects.

4. An access control system according to Claim 3, wherein a plurality of the system holders are provided, and wherein the access control server is provided for each of the system holders and is configured to issue the access permission in regard to the services provided by the service provider administrated by the system holder.

5. An access control system according to Claim 3, wherein a single access control server is provided commonly for a plurality of system holders, and is configured to

issue access permissions in regard to the services provided by the service providers administrated by the plurality of system holders.

6. An access control system according to Claim 3, further comprising a root registration authority which administrates the system holder, wherein the root registration authority is configured to execute, based on a request from the system holder, a processing to request the public key certificate issuer authority to issue the public key certificates of the authentication objects administrated by the root registration authority.

7. An access control system according to Claim 1, wherein the access control server generates the access permissions in a form independently usable for each of the service providers.

8. An access control system according to Claim 1, wherein the access control server generates the access permission in a form commonly usable for a plurality of service providers.

9. An access control system according to Claim 1, wherein the access control server is configured to generate

the access permission in a format which comprises:

an access-control-server-set fixed field set by the access control server;

a service-provider-set option field set by each of the service providers; and

an electronic signature field to be performed by the access control server.

10. An access control system according to Claim 9, wherein the service-provider-set option field includes identification data which indicates for each of the service receiving devices whether an access by the service receiving device is permitted, and wherein the identification data includes at least one of personal information concerning the user of the associated service receiving device, user ID, user device ID, and an access permission discrimination flag.

11. An access control system according to Claim 1, wherein the data transfer between the service provider, the service receiving device and the access control server, performed directly or indirectly through an intermediary, is executed on condition that mutual authentication has been established between the sender of the data and the receiver of the data.

12. An access control system according to Claim 1, wherein the data transfer between the service provider, the service receiving device and the access control server, performed directly or indirectly through an intermediary, transfers the data with an electronic signature of the sender added thereto.

13. An access control system according to Claim 1, wherein the service provider is a device which provides a service.

14. An access control system according to Claim 1, wherein the access control server is configured to execute an access permission changing processing for revocation of the permission set on the access permission.

15. An access control method for use in a data transfer system which transfers data by means of public-key cryptosystem based on a public key certificate issued to an authentication object by a public key issuer authority, the access control method comprising the steps of:

receiving, at a service provider, an access permission from a service receiving device, the access permission having been issued by a service control server; and

executing, based on the access permission, a

determination as to whether access requested by the service receiving device is to be permitted.

16. An access control method according to Claim 15, further comprising:

an access permission issuing step for issuing, at an access control server, an access permission which is delivered to the service receiving device and which enables identification of the service provide an access to which is permitted by the service receiving device.

17. An access control method according to Claim 15, further comprising the steps of:

receiving, at an access-control-server registration server, the access permission issuance request from the service receiving device and requesting, at the access-control-server registration server, the access control server to execute the processing for issuing an access permission.

18. An access control method according to Claim 15,

wherein the access permission issuing step is executed based on an issuance request from a service provider which is under the administration of a system holder as an organization that provides or controls contents usable by a

user terminal, contents which enables provision of services, or a service distribution infrastructure.

19. An access control method according to Claim 15, wherein the access permission issuing step generates the access permissions in a form independently usable for each of the service providers.

20. An access control method according to Claim 15, wherein the access control server generates the access permission in a form commonly usable for a plurality of service providers.

21. An access control method according to Claim 15, wherein the access permission issuing step generates the access permission of a format which comprises:

an access-control-server-set fixed field set by the access control server;

a service-provider-set option field set by each of the service providers; and

an electronic signature field to be performed by the access control server.

22. An access control method according to Claim 15, wherein the step executed by the service provider for

determining whether the access is to be permitted is executed based on identification data which determines whether the access is to be permitted for each of the service receiving devices and which is contained in the access permission, the identification data including at least one of personal information concerning the user of the associated service receiving device, user ID, user device ID, and an access permission discrimination flag.

23. An access control method according to Claim 15, wherein the data transfer between the service provider, the service receiving device and the access control server, executed directly or indirectly through an intermediary, is executed on condition that mutual authentication has been established between the sender of the data and the receiver of the data.

24. An access control method according to Claim 15, wherein the data transfer between the service provider, the service receiving device and the access control server, executed directly or indirectly through an intermediary, transfers the data with an electronic signature of the sender added thereto.

25. An access control method according to Claim 15,

further comprising an access permission changing processing executed by the access control server to revoke the permission set on the access permission.

26. A device having a data processing function, comprising:

communication processing means for executing data transfer processing;

cryptographic processing means for executing cryptographic processing on data; and

data storage means;

wherein the data storage means stores an access permission containing service provider identification data which identifies the service provider an access to which by a device ha been permitted;

the cryptographic processing means executes an electronic signature on the access permission; and

a processing for sending the access permission with the electronic signature is executed via the communication processing means.

27. A device according to Claim 26, wherein the access permission is a permission which is issued by an access control server that executes administration of control of access by the device to the service provider, and

wherein the device is configured to execute, by the cryptographic processing means, a processing for verifying the signature made by the access control server and added to aid access permission.

28. A device according to Claim 26, wherein the device is configured to store in the data storage means one or more access permissions each containing service provider identification data for a single service provider, or an access permission containing service provider identification data for a plurality of service providers, and to send, through the communication processing means, an access permission selected based on the access destination.

29. A device according to Claim 26, wherein the device is configured to execute mutual authentication between the device and the service provider to which the access permission is directed and to execute, on condition of the establishment of the authentication, a processing for encrypting the access permission with the electronic signature executed thereon and sending the encrypted access permission to the service provider.

30. An access control server which executes a processing for issuing an access permission which indicates

that a device is permitted to access a service provider, the access control server comprising:

communication processing means for executing data transfer processing; and

cryptographic processing means for executing cryptographic processing of data;

wherein the access control server is configured to execute: a processing for receiving, through a service provider, an access permission issuance request given by a device which requests an access to the service provider;

and a processing for issuing an access permission which contains, at least, data concerning whether the device is permitted to access the service provider and an electronic signature executed by the access control server.

31. An access control server according to Claim 30, wherein the access control server is configured to execute a processing for verifying the electronic signature of the sender added to the access permission issuance request, and to execute the processing for issuing the access permission on condition that the verification of the electronic signature has been successfully achieved.

32. An access control server according to Claim 30, wherein the access control server is configured to execute a

processing for mutual authentication between the access control server and the entity which is the sender of the access permission issuance request, and to execute a processing for receiving the access permission issuance request on condition that the mutual authentication has been established.

33. An access control server according to Claim 30, wherein the access control server is configured to execute, when executing the processing for issuing the access permission, a processing for mutual authentication between the access control server and the entity which is the sender of the access permission issuance request, and to execute a processing for encrypting the access permission and sending the encrypted access permission to the entity, on condition that the mutual authentication has been established.

34. An access control server according to Claim 30, wherein the access control server is configured to execute a processing for generating and issuing an access permission containing service provider identification data for a single service provider, or an access permission containing service provider identification data for a plurality of service providers.

35. An access-control-server registration server which executes a processing for sending a request to an access control server requesting issuance of an access permission, the access control server being responsible for executing a processing for issuing an access permission indicating that a device is permitted to access a service provider, comprising:

communication processing means for executing data transfer processing; and

cryptographic processing means for executing cryptographic processing of data;

wherein the access-control-server registration server receives, through a service provider, an access permission issuance request given by a device which requests an access to the service provider;

and wherein the access-control-server registration server further executes, upon receipt of the access permission issuance request, a processing for executing an electronic signature and then executes a processing for requesting the access control server to issue the access permission.

36. An access-control-server registration server according to Claim 35, wherein the access-control-server registration server is configured to execute:

a processing for receiving the access permission issued by the access control server;

a processing for verifying the signature of the access control server that has been added to the received access permission; and

a processing for sending the received access permission to the service provider, after adding a signature of the access-control-server registration server to the access permission.

37. An access-control-server registration server according to Claim 35,

wherein the access-control-server registration server is configured to execute:

a mutual authentication processing between the access-control-server registration server and an entity which is the sender of the access permission issuance request, and a processing for receiving the access permission issuance request on condition that the authentication has been achieved.

38. A data processing apparatus serving as a service provider which accepts accesses from a plurality of devices and which provides services in response to the accesses, the data processing apparatus comprising:

communication processing means for executing a data transfer processing; and

cryptographic processing means for executing a cryptographic processing on data;

wherein the data processing apparatus is configured to execute:

a processing for receiving, from the device, an access permission accommodating a service provider identification data that identifies the service provider to which the device has been permitted to make an access; and

a processing for determining, based on the data contained in the received access permission, whether the device is to be permitted to make an access.

39. A data processing apparatus according to Claim 38, wherein the access permission is a permission which has been issued by the access control server in response to the access permission issuance request sent from the service provider and to which an electronic signature has been added by the access control server; and

wherein the data processing apparatus serving as the service provider is configured to execute a processing for verifying the electronic signature on the access permission received from the device, and a processing for permitting the device to make the access, upon confirming, through the

verification, that the access permission is a true permission issued by the access control server.

40. A data processing apparatus according to Claim 38, wherein the data processing apparatus serving as the service provider is configured to execute:

a mutual authentication processing between the data processing apparatus and the device, and a processing for receiving the access permission issuance request.

41. A data processing apparatus according to Claim 38, wherein the data processing apparatus serving as the service provider is configured to execute, when conducting the processing for transferring the access permission to said device:

a mutual authentication processing between the data processing apparatus and the device, and a processing for sending, on condition of establishment of the authentication, the access permission, after addition of a signature of the service provider and an encryption of the access permission.

42. A program storage medium which provides a computer program that runs on a computer system to implement an access control processing in a data transfer system which transfers data by means of public-key cryptosystem based on

a public key certificate issued to an authentication object by a public key issuer authority, the computer program comprising the steps of:

receiving, at a service provider, an access permission from a service receiving device, the access permission having been issued by a service control server; and

executing, based on the access permission, a determination as to whether access requested by the service receiving device is to be permitted.